APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/773,716	01/31/2001	Masayuki Chatani	375.07.01	7005

25920   7590   06/14/2004

MARTINE & PENILLA, LLP
710 LAKEWAY DRIVE
SUITE 170
SUNNYVALE, CA 94085

EXAMINER
COLIN, CARL G

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 06/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _31 January 2001_ .

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1-53_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) _1-53_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☒ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on _31 January 2004_ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _1/22/03_ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1.   Pursuant to USC 131, claims 1-53 are presented for examination.

Specification

2.   The disclosure is objected to because of the following informalities: on page 29, line 21,

the phrase serial number is repeated before playblack. Appropriate correction is required.

Claim Objections

3.   **Claims 36-37 and 44-45** are objected to because of the following informalities: in order

to avoid rendering the claim indefinite, the term "capable of" should be corrected. Appropriate

correction is required.

Claim Rejections - 35 USC § 102

4.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another
filed in the United States before the invention thereof by the applicant for patent, or on an
international application by another who has fulfilled the requirements of paragraphs (1),
(2), and (4) of section 371(c) of this title before the invention thereof by the applicant for
patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999

(AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002

do not apply when the reference is a U.S. patent resulting directly or indirectly from an

international application filed before November 29, 2000. Therefore, the prior art date of the

reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA

35 U.S.C. 102(e)).

4.1   **Claims 1-3, 5-53** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent

6,470,085 to **Uranaka et al.**.

4.2   **As per claims 1 and 28, Uranaka et al.** discloses a method for distributing a software

product, comprising the steps of: encoding the software product with an encryption data string

for playback on a client console having a storage media detachably installed therein, for example

(see column 2, lines 20-67); receiving user identification data from a user using the client

console, for example (see column 2, lines 20-67 and column 8, lines 45 et seq.); transmitting a

first encryption key to the user, for example (see column 2, lines 20-67 and column 5, line 43

through column 6, line 65); coding an identification for the software product in the first

encryption key; receiving software product purchase information from the user, for example (see

column 2, lines 20-67 and column 5, line 43 through column 6, line 65); encoding data

representing the user purchase information and the first encryption key and a second encryption

key, for example (see column 2, lines 20-67 and column 5, line 43 through column 6, line 65);

and transmitting the first encryption key and second encryption key to the user to allow the user

to decrypt the encrypted software product, for example (see column 2, lines 20-67 and column 5,

line 43 through column 6, line 65).

As per claim 12, **Uranaka et al.** discloses a system for providing access to restricted use of digital software products, a server network comprising a server computer, a customer database storing user information, and a content database storing a plurality of software product titles, for example (see column 7, line 58 through column 8, line 42); a client console, operated by a user and configured to playback a selection of the plurality of software product titles, for example (see column 7, lines 10-37), a detachable storage media installable in said client console, for example (see column 7, lines 10-37); said detachable storage media having a data structure thereon comprising at least one of a user identifier, wherein the server computer distributes a software product to a user of the client console and encrypts the software product using information comprising the user identifier and a purchase option governing use of the software product by the user, for example (see column 7, line 58 through column 8, line 42 and column 5, line 43 through column 6, line 65).

As per claim 22, **Uranaka et al.** discloses a server computer coupled to one or more client computers over a communications network, the server computer comprising: a customer database storing user information and a content database storing a plurality of software product titles to a user of a client computer of the one or more client computers upon request of the user, for example (see column 7, line 58 through column 8, line 42); an encryption module encrypting the software product using information comprising a user identifier and a purchase option governing use of the software product by the user; and a decryption module receiving decryption information from the user and providing access to the software product upon confirmation of the

decryption information, for example (see column 7, line 58 through column 8, line 42 and

column 5, line 43 through column 6, line 65).

As per claims 31 and 40, Uranaka et al. discloses a method and apparatus for limiting

use of a distributed software product executed on a user console, comprising the steps of:

encrypting the software product with a first product key of a software cryptography system, for

example (see column 5, line 58 through column 6, line 5); distributing the software product to a

user of the user console, for example (see column 5, line 58 through column 6, line 5); receiving

a first console key of a console cryptography system comprising a first and second user key

which are created on the user console, for example (see column 6, lines 42-65); encrypting a

second product key of the software cryptography system, the second product key related to the

first product key by the software cryptography system, for example (see column 5, line 58

through column 6, line 5); and transmitting the encrypted second product key to the user so that

the encrypted software product can be decrypted on the user console using the first user key, for

example (see column 5, line 58 through column 6, line 5).

As per claims 48, 50, and 52, Uranaka et al. substantially teaches a server and a method

for distributing a software product for execution on a user console, comprising of the steps of:

distributing the software product to a user of the user console, wherein the software is stored on a

detachable storage media and locked such that access is limited to an authorized user, for

example (see column 4, line 44 through column 5, line 56); receiving a media identification of

the detachable storage media, the media identification associated with each media, for example

(see column 4, line 44 through column 5, line 56); generating a key to unlock the software using

the media identification, for example (see column 14, line 14-24); and transmitting the key to the

user so that the software product can be unlocked on the user console using the key when the

user executes the software product from the detachable storage media, for example (see column

14, line 14-27 and column 16, lines 13-45).

As per claims 2, 18, 19, 23, 29, 32, 34, 35, and 41, Uranaka et al. discloses the

limitation of, wherein the software product purchase option comprises one of: purchasing the

software product for a bounded period of time or purchasing the software product for a preset

number of accesses, for example (see column 6, lines 6-42).

As per claims 3, 15, 38, and 46, Uranaka et al. discloses the limitation of further

comprising the step of establishing a communications link between the client console and a

content provider server through a bi-directional communications network, wherein the

communications link between the client console and the content provider server comprises a

computer network link over a land-based computer network, and wherein data received from the

user and transmitted to the user are transmitted over the computer network link using a

pre-established network protocol, for example (see column 4, line 44 through column 5, line 56).

As per claim 5, Uranaka et al. discloses the limitation of further comprising the step of

establishing a telephone link between the user and a content provider and wherein data received

from the user and transmitted to the user are transmitted over the telephone link, for example (see column 6, line 41 through column 7, line 20 and column 4, lines 44-65).

As per claim 6, Uranaka et al. discloses the limitation of wherein the first encryption key and second encryption key comprise part of a two-way public key/private key encryption system, for example (see column 14, line 14-27 and column 16, lines 13-45).

As per claim 7, Uranaka et al. discloses in one embodiment the limitation of using a random number that meets the recitation of wherein the second encryption key comprises a public key of the client console, for example (see column 11, line 40 through column 12, line 25).

As per claim 8, Uranaka et al. discloses the limitation of further comprising step of coding the second encryption key into a removable memory medium detachably coupled to the client console, for example (see column 14, line 14-27 and column 16, lines 13-45).

As per claim 9, Uranaka et al. discloses the limitation of further comprising step of coding the purchase information and identification information for the client console on the removable memory medium such that the purchase information and identification information is associated with the executable code comprising the software product, for example (see column 11, line 40 through column 12, line 25).

As per claim 10, Uranaka et al. discloses the limitation of wherein the client console decodes the software product using a private key corresponding to the public key of the first encryption key, for example (see column 16, lines 12-46).

As per claims 11, 21, 25, 39, and 47, Uranaka et al. discloses the limitation of wherein the client console is an interactive computer game station and the software product is a computer game executable on the client console, for example (see column 4, line 44 through column 5, line 5).

As per claims 13 and 30, Uranaka et al. discloses the limitation of wherein the user transmits decryption information to the server computer to provide access to the software product distributed to the user, for example (see column 6, line 41 through column 7, line 20).

As per claim 14, Uranaka et al. discloses the limitation of wherein the server computer distributes the software product to the user on a readable disk media, for example (see column 6, line 41 through column 7, line 20).

As per claims 16, 17, 26, and 27, Uranaka et al. discloses the limitation of wherein the user transmits the decryption information to the server computer using a telephone coupled to the server computer through a public switched telephone network, for example (see column 6, line 41 through column 7, line 20 and column 4, lines 44-65).

As per claims 20 and 24, Uranaka et al. discloses the limitation of wherein the software product is encrypted using a public key/private key encryption system, and wherein a user public key is assigned and transmitted to the user and a client console public key is assigned and coded in the detachable storage media installable in the client console, for example (see column 14, line 14-27 and column 16, lines 13-45 and column 11, line 40 through column 12, line 25).

As per claim 7, Uranaka et al. discloses in one embodiment the limitation of using a random number that meets the recitation of wherein the second encryption key comprises a public key of the client console, for example (see column 11, line 40 through column 12, line 25).

As per claims 33 and 42, Uranaka et al. discloses the limitation of encrypting the counter using the first console key, for example (see column 5, line 57 through column 6, line 5; column 6, lines 41-67; and column 14, line 5-37); encrypting the encrypted counter value using the second user key, for example (see column 5, line 57 through column 6, line 5; column 6, lines 41-67; column 14, line 5-37); transmitted the double encrypted counter value to the user allowing the user to decrypt the double encrypted counter value on the console using the first user key, for example (see column 5, line 57 through column 6, line 5; column 6, lines 41-67; column 14, lines 14-37 and column 16, lines 13-45). **Uranaka et al.** discloses a public private key encryption system and also discloses double encryption of the distributed descriptor using public/private key wherein a counter value is one of the fields associated therewith, for example (see also claims).

As per claims 36, 37, 44, and 45, Uranaka et al. discloses the limitation of

wherein the software product is programmed onto a readable medium capable of being

played in a. playback device coupled to the user console, and wherein the first console key

comprises an identifier associated with the readable medium and a serial number of the user

console, for example (see column 4, line 57 through column 5, line 5 and column 26, lines

55-67).

As per claims 49, 51, and 53, Uranaka et al. discloses the limitation of storing the key

on a memory device, for example (see column 6, lines 41-67; and column 16, lines 47-65).

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or

described as set forth in section 102 of this title, if the differences between the subject matter

sought to be patented and the prior art are such that the subject matter as a whole would have

been obvious at the time the invention was made to a person having ordinary skill in the art to

which said subject matter pertains. Patentability shall not be negatived by the manner in which

the invention was made.

5.1   **Claim 4** is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent

6,470,085 to **Uranaka et al.** in view of US Patent 5,490,216 to **Richardson, III**.

5.2   **As per claim 4, Uranaka et al.** substantially teaches a method according to claim 2, and

further teaches using off-line and on-line communication using any telecommunication channels

to permit data communication, for example (see column 4, line 44 through column 5, line 8) and

also discloses the user provides data to be transmitted to the server at least in part by

alphanumeric codes, for example (see column 6, line 65 through column 7, line 10). **Uranaka et**

al. does not explicitly disclose using a telephone keypad to enter the information. It is well

known in the art that an order can be placed with a telephone keypad to enter alphanumeric

codes. **Richardson, III** in an analogous art teaches the step of establishing a

telecommunications link between the client console and a content provider server, and wherein

data received from the user and transmitted to the user are transmitted over the

telecommunications link using a telephone connection system, and further wherein, the user

provides data to be transmitted to the server at least in part by alphanumeric codes entered into a

telephone keypad as one of other options of communicating information, for example (see

column 7, lines 20-35). Therefore, it would have been obvious to one of ordinary skill in the art

at the time the invention was made to modify the method of **Uranaka et al.** to have data received

from the user and transmitted to the user transmitted over the telecommunications link using a

telephone connection system, and further wherein, the user provides data to be transmitted to the

server at least in part by alphanumeric codes entered into a telephone keypad as taught by

Richardson, III as other options of communicating information, for example (see column 7,

lines 20-35). This modification would have been obvious because one skilled in the art would

have been motivated by the suggestions provided by **Richardson, III** so as to communicate

information to the authority off-line.

Conclusion

6.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure as the art discloses the use of public/private key pairs to for securely distributing data

between a user and a server.

US Patent Publications: US 2003/0032486   Elliott

                              US 2002/0082997   Kobata et al.

US Patent :   6,694,025   Epstein et al.

6.1   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Carl Colin whose telephone number is 703-305-0355. The

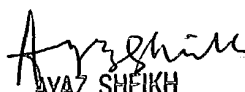examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding

should be directed to the receptionist whose telephone number is 703-305-3900.

Carl Colin

Carl Colin

Patent Examiner

June 8, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100